Tema 3: Encaminamiento Dinamico de Unidifusion y MPLS.

1. Estrategias de Encaminamiento.

Hay dos estrategias de encaminamiento en Internet:

- **ESTATICAS:** Se basan en unas rutas fijas establecidas de antemano y en donde las decisiones o informaciones encaminamiento se determinan previamente fuera de línea y luego se cargan en los routers de la organización.

  Estas informaciones de encaminamiento no varían aunque la red si lo haga, estas estrategias no se adaptan a los cambios que pueda sufrir la red durante su funcionamiento.

- **DINAMICAS:** Se basan en unas rutas dinámicas, no establecidas de antemano, y en donde las informaciones de encaminamiento varían en la medida en que lo haga la red.
  Las estrategias se adaptan a los cambios que pueda sufrir la red durante su funcionamiento.

Cuando se tenemos un gran número de enlaces por cada router es impensable una configuración manual (estática) de la tabla IP de cada router.
La configuración automática (dinámica) de la tabla de encaminamiento se utiliza sólo para organizaciones que dispongan de un número elevado de routers. Es el caso de operadores con redes IP formadas por "n" routers que tienen que intercambiar información de encaminamiento con otros operadores.
Con un solo router la configuración puede ser manual.

- **ROUTERS DINAMICOS:**

  Routers basados en una estrategia de encaminamiento dinámica. Estos routers pueden utilizar diferentes protocolos basados en diferentes algoritmos, estos algoritmos son:

  - **VECTOR DE DISTANCIAS (BELLMAN Y FORD):**

    Usa una métrica basada en el número de saltos o número de routers que hay que atravesar hasta llegar a un destino.

    Se asocia un mismo coste a cada enlace con una métrica de cuenta de saltos (normalmente 1), es decir, a cada salto en la red se la asigna un coste de salto de 1.

    > METRICA TOTAL A UN DESTINO = COSTE TOTAL A UN DESTINO = DISTANCIA A UN DESTINO = SUMA DE COSTES DE CADA SALTO

    Cada router intercambia con sus vecinos una copia de su vector de distancias, este vector incluye todos los destinos conocidos en una organización el cual está asociado con cada destino prefijado en el mensaje de encaminamiento. Esto hace que los mensajes intercambiados, salvo en el inicio, sean generalmente grandes.

    Se pueden producir bucles y para su resolución la métrica tiene un límite, por encima del límite los destinos se vuelven inalcanzables.

    Se usa en protocolos simples y sencillos, además de en organizaciones pequeñas con un número reducido de routers.

    Las tablas de encaminamiento se actualizan con lentitud, lo que hace que los mensajes se difundan con lentitud. Las rutas también se restablecen con lentitud.

- **ESTADO DE ENLACE O SPF (PRIMER CAMINO MAS CORTO):**

  Usa una métrica de enlace basada en asociar un coste igual o diferente a cada enlace para calcular posteriormente la ruta de coste mínimo.

  Esta métrica puede usar distintas medidas como el ancho de banda, retardos, longitud del enlace, paquetes encolados,…. Por tanto no va a haber límite en el número de saltos.

  > METRICA TOTAL A UN DESTINO = COSTE TOTAL A UN DESTINO = RUTA DE COSTE MINIMO AL DESTINO = SUMA MENOR DE LOS COSTES DE CADA SALTO

  Los routers que ejecutan este tipo de protocolos no intercambian tablas de encaminamiento, solo intercambian información sobre en laces y maquinas en el correspondiente dominio de encaminamiento. Esto hace que los mensajes intercambiados sean generalmente cortos.

  *DOMINIO DE ENCAMINAMIENTO: Conjunto de routers vecinos y no vecinos dentro de una organización que ejecutan un mismo protocolo de actualización y distribución de la información de encaminamiento.

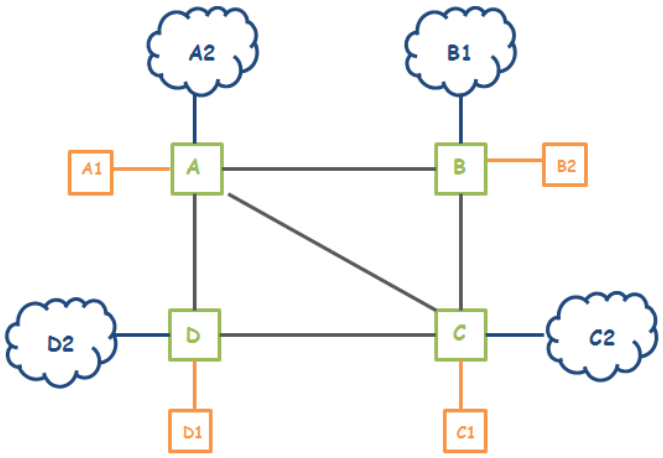
  Las tablas de encaminamiento se actualizan más rápidamente.

  Se usa en protocolos más complejos y en organizaciones grandes con un número elevado de routers.

- **ACTUALIZACION DE LA T. DE ENCAMINAMIENTO DE UN ROUTER.** Un router va a actualizar su tabla de encaminamiento cuando aparece:

  1. DESTINO NUEVO (Red o maquina)
  2. Una DISTANCIA MAS CORTA a un destino a través de otro router vecino ya insertado o no en la tabla para dicho destino.
  3. Una DISTANCIA MAS LARGA a un destino a través de otro router vecino ya incluido en la tabla para dicho destino, siempre y cuando, no aparezca otra ruta más corta al mismo destino a través de otro router vecino diferente.

  - **VECTOR DE DISTANCIAS:** Métrica = numero de saltos.



B

DESTINO	DISTANCIA	RUTA
B1	1	B
B2	1	B
A1	2	A
A2	2	A
C1	2	C
C2	2	C
D1	3	C
D2	3	C

Los destinos pueden ser direcciones de red o subred o direcciones particulares de máquina de usuario.

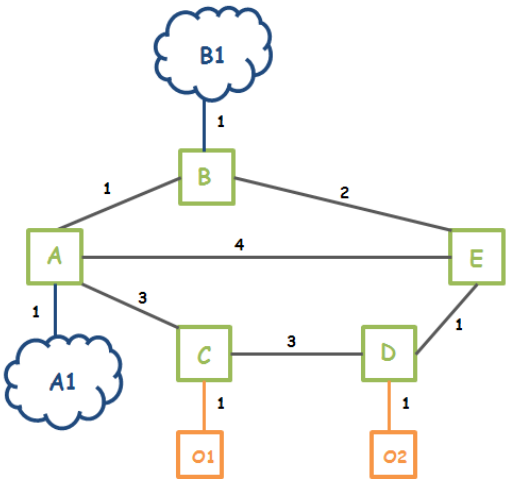
La distancia es 1 cuando aparece un routers hasta el destino.

La ruta indica el siguiente router vecino hasta llegar un destino en particular.

Inicialmente cada router solo conoce la distancia (numero de routers) a los destinos a los cuales está directamente conectado. A continuación una copia completa de esta información se intercambia por difusión o por inundación entre todos los routers vecinos.

* PROBLEMAS: Los mensajes son generalmente grandes y se difunden lentamente. Si el numero de routers es elevado se puede dar una gran sobrecarga en la red.

- **ESTADO DE ENLACE:** Para calcular el coste de un destino conectado directamente a un router no vecino hay que calcular todos los costes pasando por todos los routers vecinos.



A

DESTINO	COSTE	RUTA
O1	4	C
O2	5	B
A1	1	A
B1	2	B
B	1	B
C	3	C
D	4	B
E	3	B

Los destinos pueden ser direcciones de red o subred o direcciones particulares de máquina de usuario. Asimismo, se consideran como destinos al resto de los routers de la organización ya que en este tipo de protocolos se debe tener un conocimiento completo de toda la topología de la organización.
La distancia es 1 cuando aparece un routers hasta el destino.
El coste puede usar diferentes métricas y es el administrador de la organización quien decide su selección y asignación a cada enlace. El coste asignado a cada enlace en función de la métrica seleccionada puede ser igual o diferente.
La ruta indica el siguiente router vecino hasta llegar un destino en particular.
Para calcular el coste a un destino de un router no vecino hay que calcular todos los costes pasando por todos sus routers vecinos. Inicialmente, cada router sólo conoce el coste a los destinos a los cuales está directamente conectado. Después una copia de esta información se intercambia entre todos los routers vecinos.

1.1. SISTEMAS AUTONOMOS.

Tienen como objetivo proporcionar una visión más estructurada mediante redes más pequeñas y gestionables.

Un **SISTEMA AUTONOMO (SA)** es un conjunto de routers controlados por una única autoridad administrativa.

Estos routers se utilizan en un mismo **DOMINIO DE ENCAMINAMIENTO**. Utilizan un mismo protocolo interno (**IGP**) para la distribución y actualización de la información de encaminamiento. Generalmente un SA dispone de un único dominio de encaminamiento.

Un SA se conecta con otros SA mediante routers externos que utilizan un mismo protocolo externo (**EGP**). De esta forma, se van conectando todos los SA en Internet y, además, se controla la expansión de las tablas de encaminamiento.

Los SA suelen ser operadores con redes propias que gestionan sus propias políticas de encaminamiento y conectividad para un tráfico elevado.

Todo SA dispone de un **NUMERO DE IDENTIFICADOR** (16 bits). Se usa como un índice para la información que se utiliza para definir su política de encaminamiento. Un número de SA puede asignar, de varias formas:

1. Para los SA públicos se usa un registro delegado en Internet (RIPE NCC).
2. Para los SA privados se usa un proveedor de servicios (ISP). Los router de una organización forman un SA privado cuando intercambian información de encaminamiento entre ellos, pero no con otros. Existe un rango de números de SA reservados para SA privados, los números entre 64512 y 65535 están reservados para IANA/ICANN.
3. A través de más de un ISP. Se asume que una organización puede contar con múltiples ISP y permite tráfico de transito o no a través de dicha organización.

- **CONECTIVIDAD ENTRE LOS SA:** Internet está formado por múltiples SA.

  El grado de conectividad entre los SA es muy variable, como mínimo tienen que haber 2 SA. Un SA puede ser miembro de varios puntos neutros a través de los cuales se puede conectar con un número muy elevado de otros SA.

  Un punto neutro facilita el intercambio de tráfico nacional de Internet entre operadores.

  La conectividad entre los SA suele estar basada en dos métodos:

  - **POR TRANSITO:**

    Dos SA guardan una relación de transito si los paquetes destinados al SA "B" pueden encaminarse a través del SA "A" y viceversa.

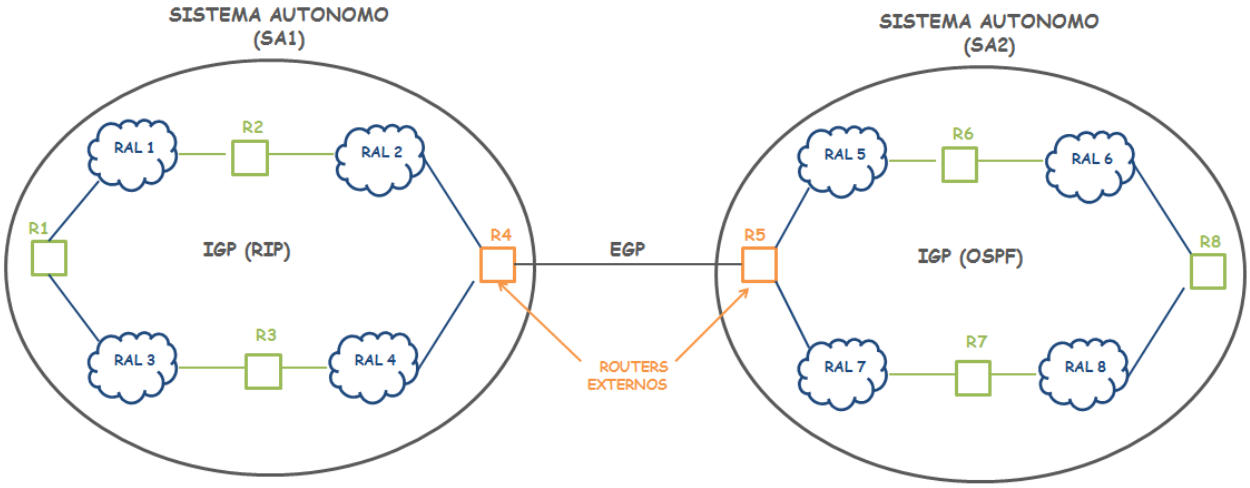
    Las rutas se publican abiertamente (vía BGP) a todos los SA y suelen incluir alguna compensación económica.

  - **POR PEERING:**

    También llamado enlace entre SA pares o "amigos". Es un enlace directo mediante una relación de transito gratuita que mantienen dos SA contiguos o pares.

    Las rutas no se publican abiertamente y permanecen en secreto (vía BGP) entre los SA "A" y "B" de tal manera que los otros SA no pueden encaminar paquetes a "B" a través de "A" ni al revés.

2. Protocolos Especificos en Internet.



Si el objetivo es poder encaminar datagramas IP en un mismo dominio desde una maquina de una red de un SA a otra máquina remota en el mismo SA, los routers usan un mismo protocolo de router interno (**IGP**) que posteriormente el protocolo IP utilizara para realizar sus funciones de encaminamiento.

Si se desean encaminar datagramas IP desde una maquina de una red de un SA a otra máquina de otro SA, los SA se conectan entre sí mediante routers externos que usan un mismo protocolo de router externo (**EGP**) a su vez y posteriormente, el protocolo IP utilizara para realizar sus funciones de encaminamiento.

Todo ROUTER EXTERNO dispone de al menos dos tablas de encaminamiento, una tabla de encaminamiento interna y otra externa. En el caso de que hubiera más de un dominio de encaminamiento, tendríamos tantas tablas de encaminamiento interno como dominios.

- **TABLA DE ENCAMINAMIENTO INTERNA:** Mantenida por el protocolo IGP para encaminar internamente por un dominio específico del propio SA.

  Todos los routers internos pertenecientes a un dominio de encaminamiento de un SA solo disponen de una única tabla de encaminamiento interna actualizada por el IGP de dicho dominio.

- **TABLA DE ENCAMINAMIENTO EXTERNA:** Mantenida por el correspondiente protocolo externo para encaminar hacia otro SA.

  Si un SA está conectado a un numero "n" de sistemas SA, un router externo tendrá tantas tablas de encaminamiento externo como sistemas SA.

- **IGP:** Protocolo interno de encaminamiento que se utiliza internamente para intercambiar información entre los routers de un dominio de encaminamiento de un SA.
  Cada SA puede ejecutar su propio conjunto de protocolos de IGP independientemente de los IGP de otros SA. El administrador de un SA tiene total libertad a la hora de seleccionar uno u otro en función de sus requisitos internos.

  - **RIP:** Se basa en la estrategia de vector distancia.
    Normalizado y aprobado para un SA en Internet por ISCO/LAB. Es el IGP más popular, especialmente, en un SA con un número reducido de routers.
  - **IGRP:** Se basa en la estrategia de vector distancia.
    Protocolo propietario del fabricante de routers Cisco y que representa una versión mejorada del protocolo RIP.
  - EIGRP: Se basa en la estrategia de vector de distancias. Es el IGRP mejorado de Cisco.
  - **OSPF**: Se basa en la estrategia de estado del enlace.
    Normalizado y aprobado para un SA en Internet por ISOC/LAB. Se puede utilizar en cualquier SA, pero esta especialmente diseñado para un SA con un número grande de routers.
  - **IS-IS:** Se basa en la estrategia de estado del enlace.
    Protocolo normalizado y aprobado por ISO para su propio protocolo de encaminamiento no orientado a conexión. Se puede utilizar para distribuir y actualizar la información de encaminamiento en una red OSI y en una red TCP/IP.

- **EGP:** Protocolo externo de encaminamiento usado externamente para intercambiar información de encaminamiento entre los SA.
  En los protocolos EGP debe haber un estándar cuando se atraviesan los SA de las organizaciones y los proveedores. Actualmente el estándar en Internet es el protocolo BGP que se basa en la estrategia de vector de distancia.
  - **BGP:** Se basa en la estrategia de vector distancia.
    Normalizado y aprobado para un SA en Internet por ISCO/LAB. Es el EGP utilizado para un encaminamiento dinámico entre los SA de Internet.

2.1 Protocolo RIPv2.

Ubicado en el nivel de aplicación por encima de **UDP** y en donde las solicitudes y respuestas se identifican a través del mismo número de puerto (520). Al estar montado UDP, RIP dispone en el nivel de aplicación de los correspondientes mecanismos fiables que UDP no proporciona.
RIP calcula las rutas usando un algoritmo de encaminamiento del vector distancia. A cada salto en la red se le asigna un coste con una métrica de cuenta de salto, normalmente 1. La métrica total a un destino es la suma de los costes de salto.
Una entidad RIP elige el siguiente salto para que los datagramas sigan un camino de coste mínimo. Un camino se considera inalcanzable cuando el número de saltos es superior a 15 para alcanzarlo.
RIP distingue entre **ROUTERS ACTIVOS**, que envían y reciben información de encaminamiento, y **ROUTERS PASIVOS**, habitualmente sistemas finales de usuario que sólo reciben información de encaminamiento.
Los routers vecinos intercambian sus tablas de encaminamiento cada 30 segundos por omisión. Si en 180 segundos no hay noticias de un router vecino se marcan todas las entradas de ese router como inalcanzables (métrica=16).
Si en dos minutos no se descubre una nueva ruta a un destino marcado como inalcanzable su entrada se elimina (**"RECOGIDA DE BASURA"**). Si por el contrario, se recibe de otro vecino un coste mínimo valido a un destino, el router reemplaza la métrica= 16 con el coste mínimo nuevo.

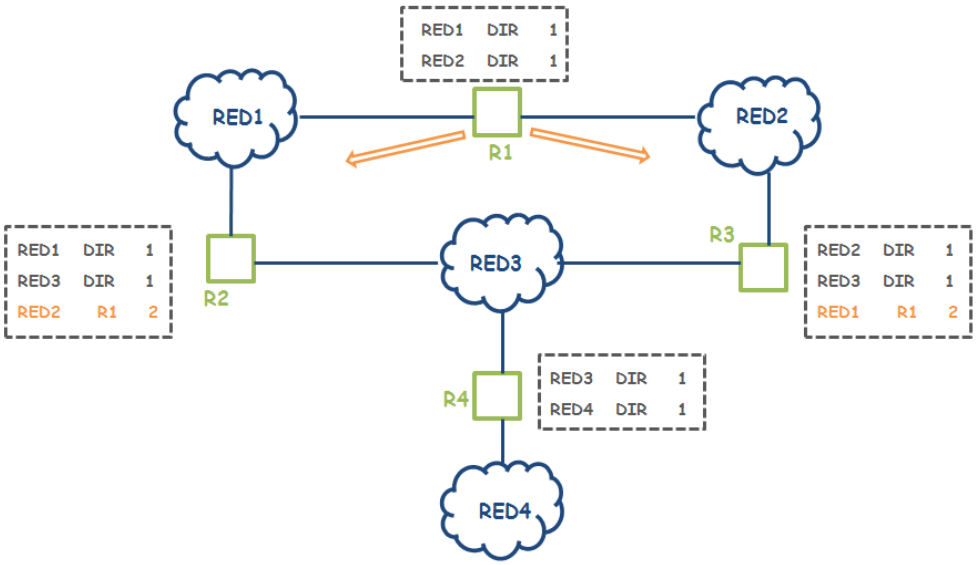
- **PROBLEMAS:** Convergencia lenta y cuenta al infinito que provocan inconsistencias en la tabla de encaminamiento. Estas inconsistencias son debido a que los mensajes de actualización son generalmente grandes con la correspondiente carga de proceso y se difunden lentamente a través de una red.

RIP es un protocolo **SENCILLO** y **MUY DISPONIBLE**, se puede encontrar en cualquier Unix. Muy útil en organizaciones pequeñas, con un número reducido de routers, o con una topología simple.

- **FUNCIONAMIENTO DEL PROTOCOLO RIP:**

Inicialmente cada router solo conoce la distancia (numero de routers) a los destinos a los que está directamente conectado.

A continuación una copia completa de esas tablas se intercambian por difusión entre todos los routers vecinos.



Al empezar R1 solo conoce los destinos RED1 y RED2 a los que está directamente conectado pasando por un único router (distancia=1) y transmite dicha información a sus vecinos (R2 y R3). Con esta última información R2 descubre un destino nuevo (RED2) al cual se accede por R1 a través de dos saltos y lo mismo ocurre con R3.

Este mismo procedimiento lo van a realizar todos los routers en orden, de manera cíclica, es decir, cuando R4 haya envía su información de encaminamiento a los demás volverá a empezar R1. Solo se van a actualizar las tablas si hay nueva información.

- **FORMATO DEL MENSAJE RIPv2:**

Un mensaje RIP consta de una secuencia de pares. Cada par consiste en una dirección IP de red y la distancia a esa dirección.

El mensaje puede contener hasta 25 entradas de direcciones. El tamaño máximo de un mensaje es de 512 octetos. Si se desea enviar más de 25 entradas, se utilizan varios mensajes. La cabecera del mensaje RIPv2 es de 20 octetos.

* **COMANDO (8 bits):** Indica si es una solicitud de información de encaminamiento (1) o una respuesta previa o una actualización espontanea (2).
* **FAMILIA DE DIRECCIONES DE LA RED (16 bits):** Identificador del formato de la dirección del nivel de red ya que el protocolo RIP puede trabajar con distintas arquitecturas de comunicación.

  Si el campo Familia de direcciones es 0xFFFF, es que lo que se está mandando es un mensaje de autenticación previo al envío de información de encaminamiento.

* **ETIQUETA DE RUTA (8 bits):** Número arbitrario que identifica a un dominio de encaminamiento dentro del mismo SA. También se utiliza para contener el número que identifica al SA. Con este campo se pretende separar rutas IP internas de rutas RIP externas que se hayan importado desde un EGP o desde otro IGP.
* **DIRECCION IP DE DESTINO (32 bits):** Dirección de red, subred o maquina de usuario.
* **MASCARA DE SUBRED (32 bits):** Mascara de la correspondiente a la dirección IP insertada en el campo etiqueta de ruta. Se admiten mascaras de longitud variable.
* **SIGUIENTE SALTO (32 bits):** Dirección del router para una ruta alternativa al destino especificado en el campo Dirección IP destino.
* **DISTANCIA AL DESTINO (METRICA) (32 bits):** Numero de saltos o routers encontrados hasta llegar al destino.

- **RIPv2 EN IPv6:** Actualmente existe un RFC-2080 que define un RIPng para IPv6, este protocolo se basa igualmente en el algoritmo del vector distancia y es similar al RIPv2 de IPv4.

2.2 Protocolo OSPFv4.

Se usa para distribuir y actualizar la información de encaminamiento entre routers dinámicos en un mismo dominio de encaminamiento de un SA, independientemente del tamaño del SA y basándose en el algoritmo de encaminamiento del estado del enlace.

Este protocolo se ubica a nivel de red, un nivel superior al IP, ya que sus paquetes se van a encapsular directamente en datagramas IP.

Permite el encaminamiento dinámico para sistemas autónomos de todos los tamaños. Acepta crecimientos en la red difundiendo rápidamente la información de encaminamiento.

OSPF introduce una jerarquía de dos niveles que permite dividir un SA en una o más **AREAS** las cuales se interconectan por un **AREA TRONCAL**. Esto proporciona una mayor escalabilidad, mayor rapidez en los cálculos y la distribución de información de encaminamiento.

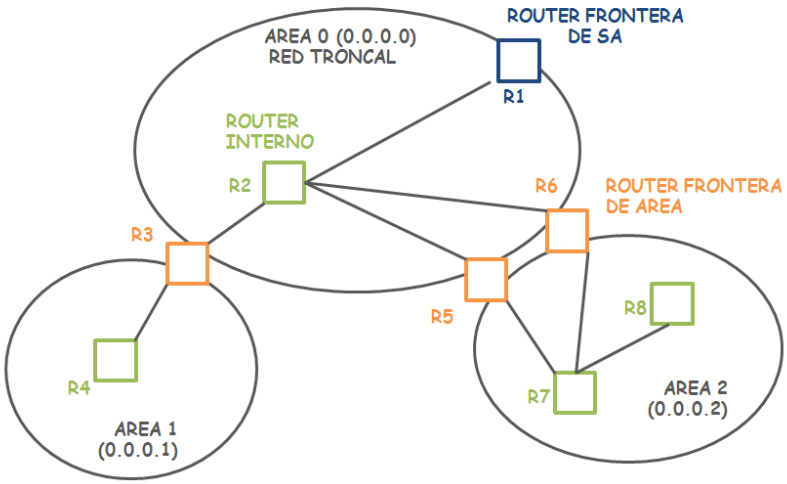
- **AREA:** Una red autónoma o un conjunto autónomo de redes contiguas. En un principio, la topología de una rea esta oculta para otras áreas.

  Todos los routers con OSPF en un área mantienen una base de datos de encaminamiento idéntica que describe la topología y estado de todos los elementos de dicha área.

  Un área se identifica con 32 bits que representa su identificador. Las distintas áreas se van a intercambiar paquetes a través del área troncal.

  - **AREA TRONCAL o AREA 0:** Parte de un SA que conecta todas las áreas de dicho SA. Transmite información de encaminamiento mediante paquetes OSPF entre las áreas del SA.

    Se identifica por el numero 0.0.0.0. Contiene todos los routers que pertenecen a múltiples áreas, así como las redes y routers no asignados a ningún área.



- **TIPO DE ROUTERS:** Cuando un SA se divide en áreas de OSPF, se definen cuatro tipos de routers.

  -**ROUTER INTERNO:** Dispositivo de encaminamiento que tiene únicamente conexiones con enlaces dentro de un solo área.

  -**ROUTER EN FRONTERA DE AREA:** Dispositivo de encaminamiento que puede estar conectado a múltiples áreas, es decir, puede tener conexiones a enlaces dentro de dos o más áreas incluyendo siempre al área 0.

  -**ROUTER TRONCAL:** Dispositivo de encaminamiento que tiene todos o parte de sus enlaces conectados al troncal. Se incluyen todos los routers que dispongan de un interfaz a más de un área.

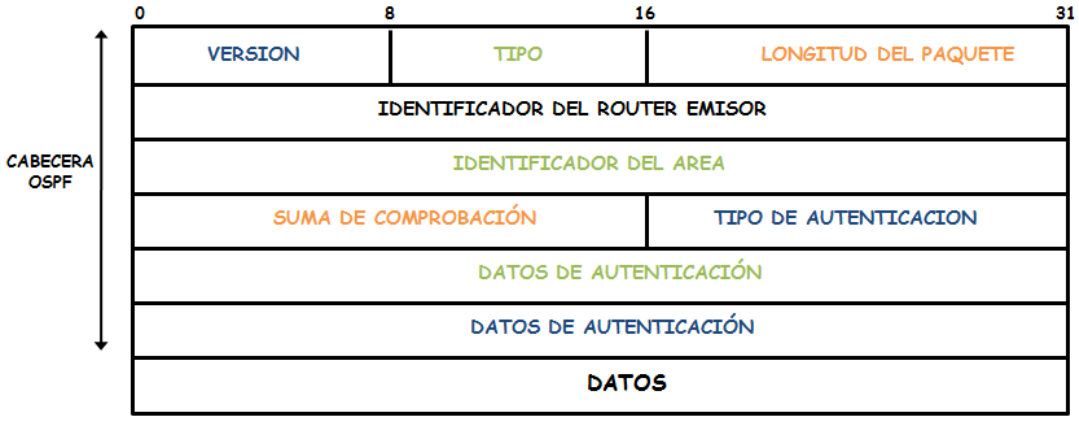
  -**ROUTER EN FRONTERA DE SA:** Dispositivo de encaminamiento limite de OSPF que tiene sus enlaces conectados a otro SA. Suponemos que el SA se conecta con el mundo exterior.
  Se comunica con otros SA en Internet a través de un EGP. Pueden ser de cualquier tipo anterior de router y además puede existir más de un router de esta tipo en un SA.

Podemos definir tres tipos de rutas en el escenario OSPF:

1. **INTRAREA:** Destino y origen se encuentran en la misma área.
2. **INTERAREA**: Cuando hay que pasar por el área 0 para llegar al destino. El origen y el destino se conectan a través del área 0.
3. **INTERSA**: El área origen y destino pertenecen a sistemas autónomos diferentes.

- **FORMATO DE UN PAQUETE OSPFv4:**

  Todo paquete OSPF consta de una cabecera fija de 24 octetos.



  * **TIPO (8 bits):** Indica el tipo de paquete OSPF. Se definen cinco tipos diferentes:

    - SALUDO (1): Permite que dos vecinos se detecten automáticamente. Paquete que se envía al arrancar y luego, periódicamente entre routers contiguos para descubrir, establecer y mantener relaciones de vecindad.

    - DESCRIPCION BASE DE DATOS (2): Paquete que intercambian los routers vecinos adyacentes para inicializar sus tablas de encaminamiento.

    - SOLICITUD DE ESTADO DE ENLACE (3): Paquete utilizado entre routers vecinos para averiguar una determinada información de encaminamiento. Se transmite cuando se ha perdido o se desean actualizar las correspondientes BBDD de estado del enlace.

    - ACTUALIZACION DEL ESTADO DEL ENLACE (4): Los envía un router mediante inundación por todos sus enlaces como respuesta a los paquetes de solicitud de estado de enlace y para informar dinámicamente de cualquier cambio en el SA.

    - CONFIRMACION DEL ESTADO DEL ENLACE (5): Paquete utilizado para confirmar la recepción de una actualización de estado del enlace. El emisor retransmitirá hasta que se confirme. Un paquete puede contener una o varias confirmaciones, una para cada aviso de estado del enlace recibido.

  * **LONGITUD DEL PAQUETE (16 bits):** Especifica la longitud total del paquete OSPF en octetos incluyendo la cabecera de OSPF.

* **IDENTIFICADOR DEL ROUTER EMISOR (32 bits):** Define al router emisor, especialmente, cuando ésta tiene más de un interfaz o dirección IP. Todos los routers están configurados con un identificador único.

* **IDENTIFICADOR DEL AREA (32 bits):** Identifica el área al que pertenece el router.

* **SUMA DE COMPROBACION (16 bits):** Detecta errores en el contenido entero del paquete OSPF, comenzando con la cabecera y siguiendo con el cuerpo del paquete.

* **TIPO AUTENTICACIÓN (16 bits) Y DATOS AUTENTICACION (64 bits):** La combinación de estos campos permite la autenticación de los pertinentes routers. Existen dos posibles valores:

  - T. AUTENTICACIÓN = 0: Sin autenticación.

  -T. AUTENTICACION = 1: Simple contraseña. La contraseña se almacena en el último campo de la cabecera denominado datos de autenticación.

- **OSPF EN IPv6:** Actualmente existe un protocolo OSPF para IPv6 definido en el documento RFC-2740.

2.3 Protocolo Bgp.

Protocolo externo usado para el encaminamiento dinámico entre routers dinámicos externos o en frontera pertenecientes a diferentes SA. Está basado en el algoritmo de encaminamiento del vector distancia.
Está ubicado en el nivel de aplicación por encima de **TCP** y en donde las solicitudes y respuestas se identifican a través del mismo número de puerto (179).
A pesar de que BGP está basado en el algoritmo de encaminamiento del vector de distancia, **NO HAY COMUNICACIÓN DE DISTANCIAS MÉTRICAS** o del número exacto de saltos que hay que realizar hasta llegar al destino.
Se usa como **MÉTRICA** el **NUMERO DE IDENTIFICADORES DE SA CONSECUTIVOS** para llegar a los destinos finales indicados. Cuantos menos identificadores aparezcan la ruta será más corta.
Revela la cadena completa de SA que hay que atravesar para llegar a un destino. Se elige siempre la cadena o ruta de SA mas corta con el menor nº de identificadores.
Desaparece el error de la formación de bucles ya que el correspondiente router externo descarta todas las rutas de los SA que pasen por él y que han sido enviadas por routers BGP vecinos.
BGP soporta el formato **CIDR** y permite la identificación de **SUPERREEDES.**
BGP contempla por omisión un servicio básico de autenticación.
Las **POLÍTICAS DE ENCAMINAMIENTO** que no forman parte de BGP se configuran estáticamente en cada router externo.

- **POLITICAS DE ENCAMINAMIENTO:** Existen herramientas para completar el uso de políticas de encaminamiento con la información de las tablas de encaminamiento. A continuación se indican algunas cuestiones que se deberían resolver por parte del administrador de un SA:

  1. **¿QUÉ RUTAS DE SA SE ANUNCIAN AL EXTERIOR Y A QUE VECINOS?**
  2. **¿QUÉ RUTAS SE ACEPTAN DESDE EL EXTERIOR Y DESDE QUE VECINOS?**
  3. **CRITERIOS DE PREFERENCIA EN CASO DE CAMINOS ALTERNATIVOS**
  4. **ENCAMINAMIENTO POR OMISION**
  5. **TIPO DE SA QUE SE VA A EMPLEAR:**

     * **SA EXTERNO:** Solo tiene una conexión InterSA con otro SA.

     * **SA MULTICONECTADO:** Dispone de conexiones con más de un SA pero se niega a transportar tráfico de transito de terceros.

     * **SA DE TRANSITO:** Dispone de conexiones con más de un SA y transporta tráfico de transito local y de terceros, pudiendo imponer políticas de transición.

- **FUNCIONAMIENTO DEL PROTOCOLO BGP:**

  Inicialmente las parejas BGP intercambian la tabla de encaminamiento de BGP completa y, después, se envían solo las actualizaciones. El protocolo BGP realiza, básicamente las siguientes funciones:

  -ADQUISICIÓN DE VECINO: Un router BGP conoce a su vecino o vecinos, es decir, un router en frontera SA se pone en contacto con los otros para intercambiar información de alcanzabilidad.

-**DETECCION DE VECINO ALCANZABLE:** Cada vecino comprueba periódicamente que su pareja BGP existe y desea mantener la relación. Verifica que los routers BGP vecinos y sus conexiones de red funcionan correctamente.

-**DETECCION DE RED ALCANZABLE:** Se transmite al correspondiente vecino la información de acceso, es decir, el anuncio o eliminación de un destino o destinos finales.

2.4 Protocolo IBGP.

La continuidad BGP dentro de un SA con otro u otros routers internos se lleva a cabo de un BGP interno o IBGP.
Cuando el numero de sesiones IBGP por encaminador es mayor que 100, se recomienda aplicar mecanismos de agrupamiento internos que permitan reducir el número de sesiones necesarias.
Se aplican distintos mecanismos como son las confederaciones.

- **CONFEDERACIONES:**
  Técnica para reducir la malla IBGP dentro de un SA. Consiste en agrupar varios SA en uno.
  Precisan de la utilización de los números reservados para los sub-SA internos que figuran en el rango 64512-65535.
  Estos números se usan internamente y pueden utilizarse en muchas otras confederaciones distintas, ya que no salen anunciados hacia fuera esos SA.

3. Conmutacion de Etiquetas Multiprotocolo (MPLS)

Tecnología de red que mejora el tratamiento del tráfico IP respecto al método convencional de encaminamiento en los routers.
El objetivo inicial es aumentar la eficiencia en el proceso de los routers mediante un mejor método de encaminamiento o reenvío.
Usa una **TECNICA DE CONMUTACION RAPIDA PARA IP** que incorpora mecanismos de otras tecnologías como **ATM** y usada en las redes actuales de los operadores.

Reenvío de paquetes sin analizar la cabecera IP.

Se pone, por delante de cada datagrama IP, una **CABECERA MPLS** adicional (32 bits) con un campo de control denominado **"ETIQUETA"** (20 bits) y el encaminamiento se realiza en función de dicha **"ETIQUETA"** y no por la dirección de destino de la cabecera IP.

La **"ETIQUETA"** simplifica el numero de tareas en el proceso del datagrama.

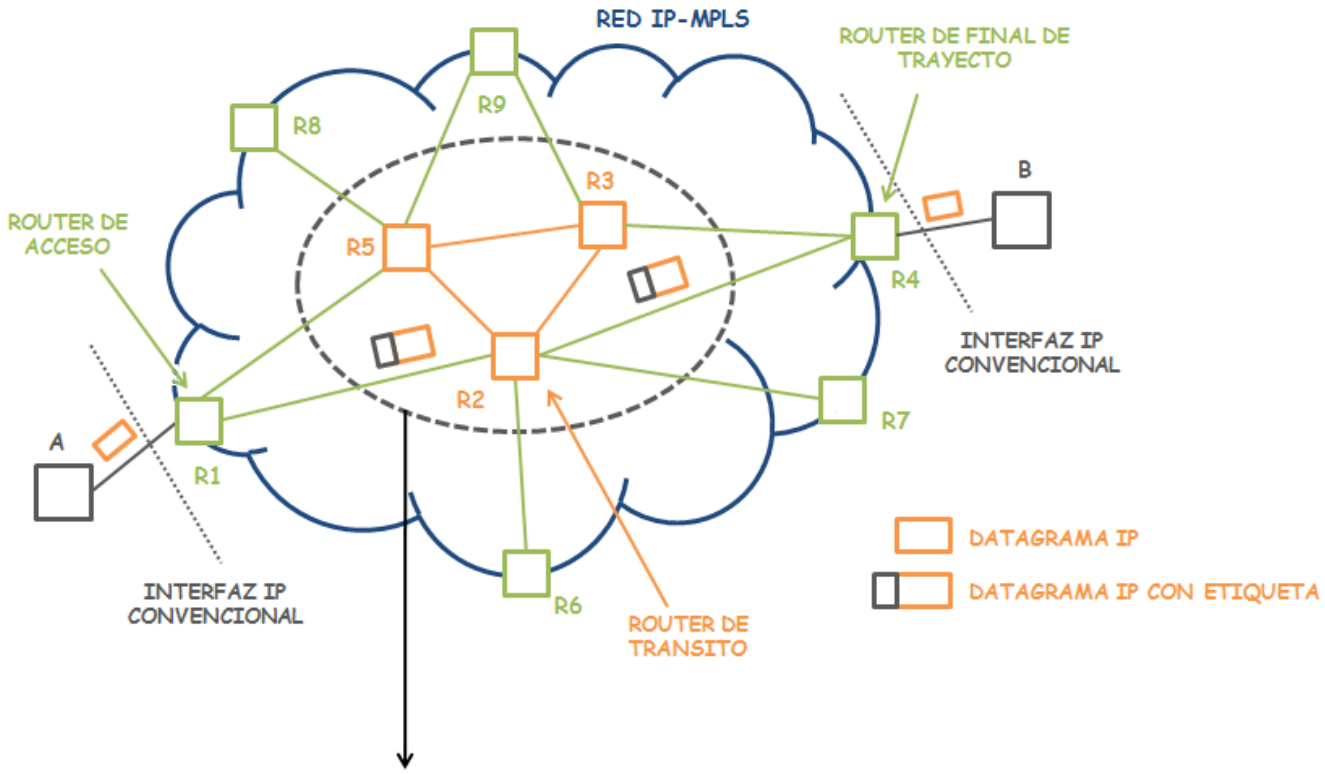
Cada **ROUTER IP-MPLS** mantiene una tabla de etiquetas con la asociación interfaz de entrada y etiqueta de entrada-interfaz de salida y etiqueta de salida.

Cada datagrama IP junto con su cabecera MPLS se encapsula directamente sobre tramas del nivel de enlace.

- **FEC (CLASE EQUIVALENTE DE RETRANSMISIÓN):**
  Conjunto de paquetes que van a recibir un mismo tratamiento.
  Todos los datagramas deben ser procesados de la misma forma desde el punto de vista del siguiente salto.

- **ROUTER O CONMUTADOR MPLS:** Router capaz de conmutar dos tipos de etiquetas:
  * **ROUTER DE ACCESO MPLS:** LER (Label Edge Router).
  * **ROUTER DE TRANSITO MPLS:** LSR (Label Switch Router)
- **DOMINIO MPLS:** Conjunto contiguo de routers con funcionalidad MPLS.

3.1 Funcionamiento Mpls.

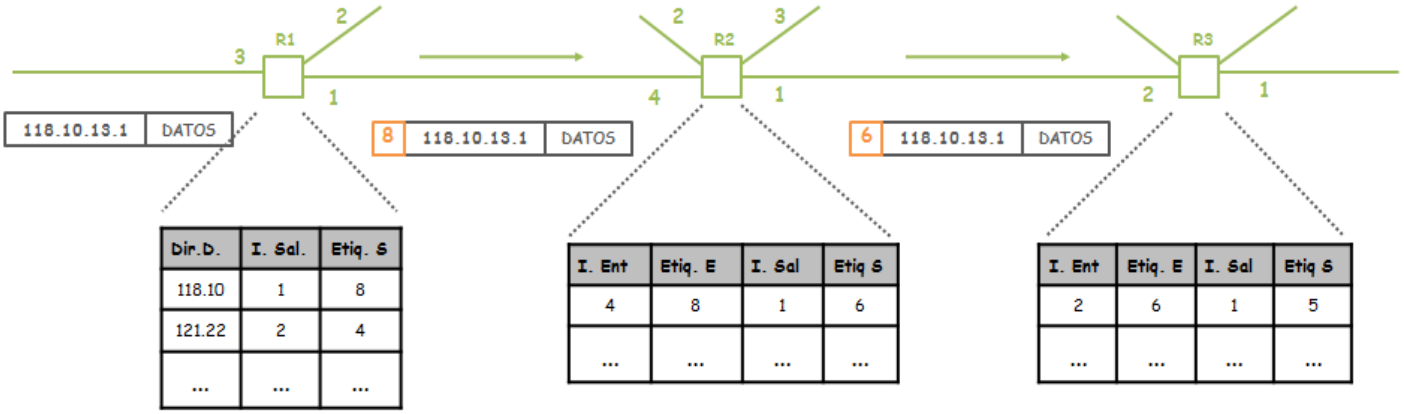


ROUTERS DEL NUCLEO CENTRAL: Disponen de tablas de encaminamiento por etiquetas para no consultar la cabecera del datagrama IP.

El router de acceso (R1) asigna una etiqueta a cada datagrama IP en los routers de acceso a la red. La cabecera del datagrama IP sólo se analiza una vez en el primer router.
Los routers de la red de transporte (routers de transito) conmutan por etiquetas.
El último router de la red acceso (router final de trayecto), R4, quita la etiqueta.

- **CONMUTACION MPLS:**

  Al llegar un datagrama IP al router de acceso, éste le añade un campo etiqueta con un valor. El siguiente router de transito consulta el campo etiqueta de entrada (E.E.) en su tabla de etiquetas buscando dicho valor para su interfaz de entrada y cambia el valor de entrada por el valor o numero etiqueta asociado en el campo etiqueta de salida (E.S.) y así sucesivamente.



Dir.D.	I. Sal.	Etiq. S
118.10	1	8
121.22	2	4
...	...	...

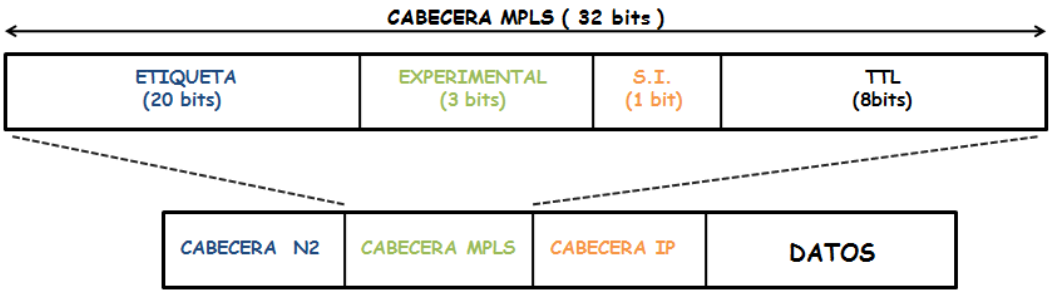
I. Ent	Etiq. E	I. Sal	Etiq S
4	8	1	6
...	...	...	...

I. Ent	Etiq. E	I. Sal	Etiq S
2	6	1	5
...	...	...	...

- **TRAYECTO MPLS (LSP, LABEL SWITCHED PATH):** Ruta definida mediante la asociación o concatenación de etiquetas o números FEC.

  Un LSP es el circuito virtual que siguen todos los paquetes pertenecientes a un mismo FEC, el cual se establece previamente antes del envío. Es la secuencia de id de las etiquetas desde el origen hasta el destino.

3.2 Cabecera Mpls.



*ETIQUETA MPLS o ETIQUETA FEC: Campo de control de la cabecera MPLS de 20 bits cuyo contenido es un número "corto" de longitud fija que identifica el valor de la etiqueta.

* S.I. (1 bit): Identificador de Pila (Stack Identifier), se encarga de diferenciar varias etiquetas.

La última etiqueta se identifica con cero.

*EXPERIMENTAL (3 bit): Para ofrecer calidad de servicio según el modelo de servicios diferenciados. Paquetes de Voz (101) y Paquetes de Datos (011)

- ETIQUETAS MPLS: Similar a un identificador de conexión o Identificador lógico Camino Virtual-Canal Virtual (VPI-VCI) de una célula ATM.

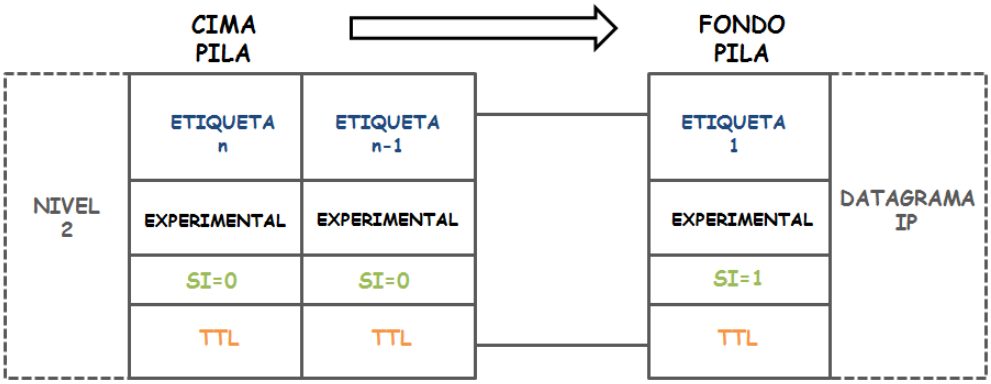
Tiene SIGNIFICADO LOCAL (la etiqueta cambia en cada router) a diferencia del significado global de la dirección IP (que no cambia en la red IP)

El primer router MPLS (router de acceso) pone una etiqueta en función de la dirección IP (prefijo) de la maquina destinataria

* ASIGNACION DE ETIQUETAS: La asignación de etiquetas se puede hacer de dos maneras: Por la dirección de red (prefijo) o en función de la aplicación.

Cada dominio MPLS va a tener una etiqueta asociada, de tal manera que en la primera entrada de cada dominio se añade una nueva etiqueta, procesándose siempre la etiqueta que está en la cima de la pila.

* JERARQUIA DE ETIQUETAS: MPLS permite el uso de varias etiquetas apiladas según la filosofía LIFO (Last In, First Out).



El bit SI activado indica que es la última etiqueta (la primera en llegar). El bit SI no activado indica que hay varias etiquetas apiladas.

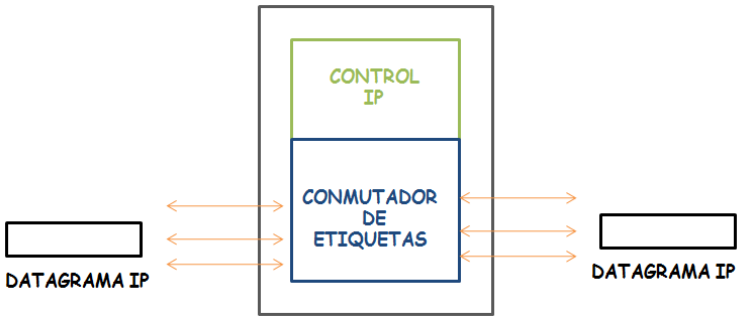
Se procesa siempre la etiqueta que está en la cima de la pila (última etiqueta que se añadió al datagrama IP)

Las etiquetas se mueven en sentido contrario a la transferencia de datos (del destino hacia el origen)

* CONTROL DE DISTRIBUCION DE ETIQUETAS ORDENADO: Cada router MPLS espera recibir la etiqueta del router descendente (Etiqueta de entrada: EE) y apunta la etiqueta recibida en la tabla de etiquetas como salida (Etiqueta de salida: ES) y realiza la asignación de una etiqueta local (EE) a dicha ES y distribuye dicha etiqueta (EE) a los routers ascendentes.

3.3 Router Ip-Mpls.

Un router MPLS es un router IP y, por tanto, dispone del protocolo IP y del correspondiente soporte de encaminamiento dinámico para construir PREVIAMENTE el trayecto de menor coste y que la solicitudes de etiquetas se hagan al router IP.MPLS vecino en la ruta más corta a la red de destino



- **CONTROL IP:** RIP, OSPF, IS-IS, BGP-4
- **CONTROL MPLS:** LDP (Label Distribution Protocol). Se usa para descubrir la presencia de router MPLS (UDP) y para crear, cambiar y borrar las asociaciones etiqueta-FEC (vía TCP)